REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

It is still believed that the claims subject to appeal did not read on a modified DES operation as taught by the Kocher publication, because Kocher does not disclose coordinating disguising of the operation *h(x)* with disguising of the input data *(x)* so that the condition $h(x) = h_{R2}(x_{R1})$ is met (*i.e.*, the result of executing the undisguised operation with undisguised data x must equal the result of executing the disguised operation with the disguised data).

Nevertheless, in order to even more clearly distinguish the invention, claims 1 and 9 have now been amended to explicitly recite the **multiple executions** referred to in lines 7-8 on page 2 of the original specification, and the **new disguising of operations and data before "*each new execution*"** as disclosed in lines 23-25 on page 2 of the original specification. In addition, the dependent claims have been amended for consistency with amended claims 1 and 9. Because the additions to the claims are supported by the original specification, it is respectfully submitted that they do not involve "new matter."

Basically, the claims now positively recite that the operation and the data are newly disguised *each* time data is to be processed using the operation, *with the correlation* $h(x) = h_{R2}(x_{R1})$ *being maintained for each newly disguised operation and data*. Kocher does not disclose a new disguising operation for each subsequent execution of an operation, in such a way that the relationship $h(x) = h_{R2}(x_{R1})$ between the *newly disguised operation* and the *newly disguised data* is maintained for each execution. Instead, Kocher's modified DES algorithm (DES(m1,k1) ¤ DES(m2,k2)) (wherein m and k are *input data*, namely messages and keys) is the **same** for each execution and is not modified to compensate for concretely disguised input data according to the relationship $h(x) = h_{R2}(x_{R1})$. In fact, the operation (DES(m1,k1) ¤ DES(m2,k2) is not disguised at all (randomizing the input data does not disguise the operation, but rather

simply disguises the input data), and is not individually adapted to compensate for concretely disguised input data.

According to the invention, an operation *(h)* and input data *(x)* is disguised so that execution of the disguised operation (h_{R1}) with the disguised input data $(x \otimes R1)$ yields the same result y as execution of execution of the original undisguised operation *(h)* with the original input data *(x)*. Thus, the invention not only disguises or randomizes the input data (Kocher's message m and key k) *each* time the operation is carried out, but also disguises the operations used to process the data *each* time the operation is carried out. Even though both the input data and the operation are disguised, however, it is desired to ultimately obtain the same result as if the input data and operation had not been disguised.[1] This is why the claimed invention requires a specific relationship between the original and disguised input data, and the original and disguised operation.

Disguising an operation, such as an encryption operation, each time the operation is carried out, is not the same as using a modified operation, such as Kocher's modified encryption operation (in which the original operation is broken up into two parts, but which then applies the same two part operation each time a new message is to be encrypted). If the modified encryption operation reaches the same result as the original encryption operation (just in a more complicated way), then it will *always* reach the same result and there is no need to coordinate original and modified input data and operations in the manner claimed. If a different result is reached, then

---

[1] This can be understood by considering that the operation might be an encryption operation. The invention assumes that the file is to be encrypted by a particular encryption operation and decrypted by a corresponding decryption operation. In order to preserve the ability of a third party to decrypt the file using the decryption operation, it is necessary that any changes to the encryption operation and original message and file must not affect the results of the encryption operation, namely the encrypted file, or the third party will not be able to decrypt the file. This would not be a problem if the encryption operation were merely modified and the same modified operation were used for each execution, as in Kocher, because the third party could simply be provided as necessary with a modified decryption operation. However, the claimed invention modifies the encryption operation, as well as the input data, before *each* execution, and therefore an added step is necessary to enable a third party to decrypt the resulting encrypted file. The added step is the step of ensuring that application of the disguised operation to the disguised data will not change the ultimate result, *i.e.*, will be the same as applying the undisguised operation to the undisguised data. This added step is not necessary in Kocher.

a different result will always be reached, and a different decryption operation must be provided to third parties wishing to decrypt the file, in which case there is still no need for the claimed coordination..

This basic principle of the invention, that in order to obtain a meaningful result a new disguised operation is required each time new data is to be processed, is set forth in lines 5-10 on page 2 of the original specification, as follows:

> *. . .For this purpose the security-relevant operations are disguised or falsified with the aid of suitable functions before execution. In order to impede or even prevent in particular a statistical evaluation in case of* ***multiple execution*** *of the security-relevant operations,* ***a random component*** *enters into the disguising function. As a result, an attacker cannot determine the secret data from any data streams intercepted.*

The Examiner will appreciate that the basic reason for disguising the operation is not that it can be discovered by analysis of signals after one pass. It is logically impossible to deduce the steps of an operation after one pass if the data is disguised and therefore unknown. The problem is that the operation can be discovered by statistical analysis of signals emitted by execution of the same operation a large number of times. The statistical analysis reveals what patterns the different executions have in common, so as to separate the contributions of the different data from the contributions of the repeated operation steps.

No matter how sophisticated the operation, it is in theory vulnerable to detection by statistical analysis of repeated executions. This is true of basic DES and of modified DES. Furthermore, this is true even though the operations use random numbers during processing. The effect of randomizing keys during processing is the same as randomizing the message or input data–so long as the sequence of operations being performed is the same and the number of executions being analyzed is sufficiently high, the operations can be deduced even if the keys or inputs to the operations are varied and/or disguised. This is why the invention not only disguises the input data, but also the operations, ***each*** **time data is to be processed**. By disguising both

the data and operations, each time using different random numbers[2], deduction of the operation by statistical analysis becomes impossible.

In contrast, as described in the Kocher patent, random values k1 ahnd m1 are produced and k2 and m2 are respectively computed as $k2 = k \otimes k1$ and $m2 = k \otimes m1$, and that in addition permutations k1p, k2p, m1p, and m2p are produced and respectively applied to k1, k2, m1, and m2. Further, "*the permuted keys and messages are then used, rather than the standard key and message, during the cours of the cryptographic operation*" (paragraph [0035]) and, "*at the end of such operation, the two parts of the cyphertext may be recombined to form the same encrypted/decrypted quantity that would have been produced by a standard DES protocol*" (paragraph [0036]). In other words, for two different sets of input data, (m1',k1'),(m2',k2') and (m1",k1"),(m2",k2"), the operation DES(-,-)¤DES(-,-) and especially the recombination operator ¤ remains the same, unlike the claimed invention where the operation h_{R1} depends on x_{R1}, and thus has to be newly modified/disguised each time the security-relevant operation h is executed.

In summary, the claims have been amended to clarify that:

(a) the operation h is actively and individually disguised each time it is executed, which is not the case in Kocher where input data may be individually disguised each execution, but not the DES algorithm, and

(b) the disguising of operation and input data are dependent on each other, which is also not the case in Kocher where new disguising of the input data (m,k) does not influence the modified DES algorithm to be executed.

As a result, Kocher neither anticipates nor discloses the invention as currently claimed, and withdrawal of the rejection under 35 USC §102(e) is respectfully requested.

---

[2] See page 2, lines 23-25 of Applicant's specification: "*Before **each new execution** of the security-relevant function one can preset **new random numbers** R_1 and R_2 from which new disguised function h_{R1R2} is determined in each case.*

Having thus overcome each of the rejections made in the Official Action, withdrawal of the rejections and expedited passage of the application to issue is requested.

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
Registration No. 33,805

Date: March 27, 2009

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500

NWB:S:\Producer\bcu\Pending Q...Z\WATER 763621\a05.wpd